

# Basic Axioms and Examples

## Note 1

cca4f1927b2c4eaa3123dbcf0680bc0

Given a set  $G$ ,  $\{\{c2:: \text{a binary operation } \star \text{ on } G\}\}$  is  $\{\{c1:: \text{a function}$

$$\star : G \times G \rightarrow G.$$

$\}\}$

## Note 2

7732d25ebb1e40dd9696c1c921803c17

Given a binary operation  $\star$  on a set  $G$ , for any  $a, b \in G$  we shall write  $\{\{c2:: a \star b\}\}$  for  $\{\{c1:: \star(a, b),.\}\}$

## Note 3

4fc60827250f4af4ab6a669ac7632568

A binary operation  $\star$  on a set  $G$  is  $\{\{c2:: \text{associative}\}\}$  if  $\{\{c1:: \text{for all } a, b, c \in G \text{ we have}$

$$a \star (b \star c) = (a \star b) \star c.$$

$\}\}$

## Note 4

192d8d86f22349cabcd9f1a229fc45290

If  $\star$  is a binary operation on a set  $G$  we say elements  $a$  and  $b$  of  $G$   $\{\{c1:: \text{commute}\}\}$  if  $\{\{c2::$

$$a \star b = b \star a.$$

$\}\}$

## Note 5

e5cbf512d6a54c91950c65450a07a501

A binary operation  $\star$  on a set  $G$  is  $\{\{c2:: \text{commutative}\}\}$  if  $\{\{c1:: \text{for all } a, b \in G \text{ we have}$

$$a \star b = b \star a.$$

$\}\}$

## Note 6

36b096eebd7f4264ab071a5fa4cfe13

Suppose that  $\star$  is a binary operation on a set  $G$  and  $H \subseteq G$ . If  $\{\{c2:: \text{the restriction of } \star \text{ to } H \text{ is a binary operation on } H,\}\}$  then  $H$  is said to be  $\{\{c1:: \text{closed under } \star,\}\}$

## Note 7

644b1cd8fa014885ad295ae5c089e5a7

A group is an ordered pair  $(G, \star)$  where  $G$  is a set and  $\star$  is a binary operation on  $G$  satisfying the group axioms.

## Note 8

5de4e717b4814adf8acd4f8d9a93322c

How many axiom are there in the definition of a group  $(G, \star)$ ?

■ Three.

## Note 9

2dc690f5008a4b8c8691c36308e44295

What is the first axiom from the definition of a group  $(G, \star)$ ?

■  $\star$  is associative.

## Note 10

4fcc137e66a048459cc73d6735e4ccea

Given a binary operation  $\star$  on a set  $G$ , an element  $e \in G$  is called an identity of  $G$  if for all  $a \in G$  we have

$$a \star e = e \star a = a.$$

}

## Note 11

a3cd125f152f432082757242096a76ef

What is the second axiom from the definition of a group  $(G, \star)$ ?

■ There exists an identity of  $G$ .

## Note 12

5d438f0c3fb24b1a97507e81f868846e

Given a binary operation  $\star$  on a set  $G$  and  $a \in G$ , an element  $\tilde{a} \in G$  is called an inverse of  $a$  if

$$a \star \tilde{a} = \tilde{a} \star a = e.$$

}

### Note 13

d840b7b910d740f3bea231c74feba51c

Given a binary operation  $\star$  on a set  $G$  and  $a \in G$ , an inverse of  $a$  is usually denoted  $a^{-1}$ .

### Note 14

c4c56a11c6f746b3ae287ec386b4e12b

What is the third axiom from the definition of a group  $(G, \star)$ ?

■ For all  $a \in G$  there exists  $a^{-1}$ .

### Note 15

be05e23d350d4f49a65602b65045f888

A group  $(G, \star)$  is called abelian if  $\star$  is commutative.

### Note 16

978f23382d594a28a3de168b7f661c30

We shall say  $G$  is a group under  $\star$  if  $(G, \star)$  is a group.

### Note 17

497f01593d7f4ffabb546b455788b354

We shall say a set  $G$  is a group if  $G$  is a group under an operation that is clear from the context.

### Note 18

61ea2504ca474fe4aae902eb1965576c

$\mathbb{Z}, \mathbb{Q}, \mathbb{R}$  and  $\mathbb{C}$  are groups under  $+$ .

### Note 19

84b6a231d3934ab3b4f63226549a9589

$\mathbb{Q} - \{0\}, \mathbb{R} - \{0\}, \mathbb{C} - \{0\}$  are groups under  $\times$ .

### Note 20

3051cd354f5040e2bdf0809e005635ed

$\mathbb{Q}^+, \mathbb{R}^+$  are groups under  $\times$ .

### Note 21

21f924e833cd4e0bbae5f4588dff47b5

Is  $\mathbb{Z} - \{0\}$  a group under  $\times$ ?

■ No. (There is no inverse.)

## Note 22

edec2a960f6d43dbb5e19283c28db7bd

Let  $V$  be a vector space. Then  $V$  is  $\{\{c2: \text{a group}\} \text{ under } \{\{c1: +, \cdot\}\}$

## Note 23

47a03e2c688244b1b3a5126fd04a21c7

Let  $n \in \mathbb{Z}^+$ . Then  $\{\{c3: \mathbb{Z}/n\mathbb{Z}\} \text{ is } \{\{c2: \text{a group}\} \text{ under } \{\{c1: \text{addition}\}\} \text{ of residue classes.}$

## Note 24

f6a5a40cfee6495dae0d36f7b3288cb2

Let  $n \in \mathbb{Z}^+$ . Then  $\{\{c3: (\mathbb{Z}/n\mathbb{Z})^\times\} \text{ is } \{\{c2: \text{a group}\} \text{ under } \{\{c1: \text{multiplication}\}\} \text{ of residue classes.}$

## Note 25

3e94ca73ca344269bb98d94a22204fd9

If  $(A, \star)$  and  $(B, \diamond)$  are  $\{\{c4: \text{groups},\} \text{ then the group } \{\{c2: A \times B,\} \text{ whose operation is } \{\{c1: \text{defined componentwise:}$

$$(a, b)(c, d) = (a \star c, b \diamond d),$$

$\} \text{ is called } \{\{c3: \text{the direct product of the two groups.}\}$

## Note 26

e23d8e577b3948af9b0cadd5df7c9141

If  $(G, \star)$  is a group, then  $\{\{c2: \text{the identity of } G\} \text{ is } \{\{c1: \text{unique.}\}$

## Note 27

5b5391986e9b49ea9c5f9f73813e9594

If  $(G, \star)$  is a group, then the identity of  $G$  is unique. What is the key idea in the proof?

■ Consider the product of two arbitrary identities.

## Note 28

0989a259fae446c48bb0f6c40394efd0

If  $(G, \star)$  is a group, then for every  $a \in G$ ,  $\{\{c2: a^{-1}\} \text{ is } \{\{c1: \text{uniquely determined.}\}$

### Note 29

f0b0a651592c466ba8067beb3b1570b8

If  $(G, \star)$  is a group, then for every  $a \in G$ ,  $a^{-1}$  is uniquely determined. What is the key idea in the proof?

■ Multiply an inverse on the right by  $a \star a^{-1}$ .

### Note 30

4a6a6806d8874839bb7956d76e384333

If  $(G, \star)$  is a group and  $a \in G$ , then

$$(a^{-1})^{-1} = \{\{c1::a.\}\}$$

### Note 31

9ab0e972d6a24baea99f1577cbf03423

If  $(G, \star)$  is a group and  $a, b \in G$ , then

$$\{\{c2::(a \star b)^{-1}\}\} = \{\{c1::(b^{-1}) \star (a^{-1}).\}\}$$

### Note 32

69b3db6e70ad4629aa55a855b8df8096

If  $(G, \star)$  is a group and  $a_1, \dots, a_n \in G$ , then the value of

$$a_1 \star \dots \star a_n$$

is  $\{\{c2::\text{independent}\}\}$  of  $\{\{c1::\text{how the expression is bracketed.}\}\}$

« $\{\{c3::\text{The generalized associative law}\}\}$ »

### Note 33

05cc8fd523084650adb46704dde222a7

What is the key idea in the proof of the generalized associative law for a group  $(G, \star)$ ?

■ By induction.

### Note 34

9ca193d1531c4c49b296732d7ff12fb5

Henceforth our abstract groups  $G, H$ , *etc.* will always be written with the operation as  $\{\{c1::\star.\}\}$

### Note 35

7d06acac21c14a628ad1ccb470fe6398

Henceforth for an abstract group  $G$  (operation  $\cdot$ ) an expression  $\{\{c2::a \cdot b\}\}$  will always be written as  $\{\{c1::ab\}\}$

### Note 36

0994e6080f3042ad81bc90d1ced0b747

Henceforth for an abstract group  $G$  (operation  $\cdot$ ) we denote  $\{\{c2::$  the identity of  $G\}\}$  by  $\{\{c1::1\}\}$

### Note 37

361c99f13a9b4304868fdb350b45dbf

For any group  $G$  and  $x \in G$  and  $\{\{c3::n \in \mathbb{Z}^+\}\}$  we shall denote by  $\{\{c2::x^n\}\}$   $\{\{c1::$  the product

$$\underbrace{xx \cdots x}_{n \text{ terms}}$$

$\}\}$

### Note 38

5b7f3c41cf0147e2bffc3929ed9ec480

For any group  $G$  and  $x \in G$  and  $\{\{c3::n \in \mathbb{Z}^+\}\}$  we shall denote by  $\{\{c2::x^{-n}\}\}$   $\{\{c1::$  the product

$$\underbrace{x^{-1}x^{-1} \cdots x^{-1}}_{n \text{ terms}}.$$

$\}\}$

### Note 39

a7a44229ce0f4a4b11d1410dc0fab0f

For any group  $G$  and  $\{\{c3::x \in G\}\}$  let  $x^{\{\{c2::0\}\}} \stackrel{\text{def}}{=} \{\{c1::1, \text{ the identity of } G\}\}$ .

### Note 40

b1be1b97f53c45fa9451caa7112ca406

Let  $G$  be a group and let  $a, u, v \in G$ . Then  $au = av$   $\{\{c2::$  if and only if  $\}\}$   $\{\{c1::u = v\}\}$

« $\{\{c3::$  Cancellation rule $\}\}$ »

### Note 41

ed8673154d544c7b86ac358facc79101

For  $G$  a group and  $x \in G$  define the order of  $x$  to be the smallest positive integer  $n$  such that

$$x^n = 1.$$

}}

### Note 42

8c334a6360be4bec8fae7f712ab2c4ee

For  $G$  a group and  $x \in G$ , if no positive power of  $x$  is the identity, the order of  $x$  is defined to be infinity.

### Note 43

ba4143a322564f8383f6e7d91ca32a75

For  $G$  a group and  $x \in G$ , denote the order of  $x$  by  $|x|$ .

### Note 44

d7fee5bcbdbd47bcb6f4a2ba086fa2ed

For  $G$  a group and  $x \in G$ , if the order of  $x$  is an integer  $n$ ,  $x$  is said to be of order  $n$ .

### Note 45

db12c606699d40e89d499d554bd52b28

For  $G$  a group and  $x \in G$ , if the order of  $x$  is infinite,  $x$  is said to be of infinite order.

### Note 46

2e514c62ce4e48eb9c6bd3b5de1d7c44

An element of a group has order 1 if and only if it is the identity.

### Note 47

babeb7cf1b394be6a4f8d86e1a099cda

Let  $G = \{g_1, g_2, \dots, g_n\}$  be a finite group with  $g_1 = 1$ . The multiplication table or group table of  $G$  is the matrix

$$[g_i g_j] \sim n \times n.$$

}}

**Note 48**

f245736b42b44f178f9a1d661bc4a5c7

Let  $G = \{x \in \mathbb{R} \mid x \in [0, 1)\}$  and for  $x, y \in G$  let  $x \star y$  be the fractional part of  $x + y$ . Then the group  $(G, \star)$  is called the real numbers mod 1.

**Note 49**

3664191737c844f38816547b7acd64c1

Let  $G = \{z \in \mathbb{C} \mid z^n = 1 \text{ for some } n \in \mathbb{Z}^+\}$ . Then the group  $(G, +)$  is called the group of roots of unity in  $\mathbb{C}$ .

**Note 50**

85c981d4f1564164bb547096829d245b

A finite group is abelian if and only if its group table is a symmetric matrix.

**Note 51**

859ef5188ad14b35b58dc9428333e5ad

Let  $G$  a group and  $x \in G$  and  $a, b \in \mathbb{Z}$ . Then  $x^{a+b} = x^a x^b$ .

**Note 52**

0c6c419e61fc48139ff6afd4a8e28be6

Let  $G$  a group and  $x \in G$ . Then  $|x^{-1}| = |x|$ .

**Note 53**

f221410dc76e4c7881175d62226ecd4

Let  $G$  a group and  $x, g \in G$ . Then  $|g^{-1}xg| = |x|$ .

**Note 54**

9951f3d62ec841df9c6f8cfc07f3c04f

Let  $G$  a group and  $a, b \in G$ . Then  $|ba| = |ab|$ .

**Note 55**

b30a94de99fe4c2f91b5417fdbb3e99d

Let  $G$  a group,  $x \in G$ ,  $|x| = n < \infty$  and  $s \in \mathbb{Z}$ . Then  $x^s = 1$  if and only if  $n \mid s$ .

**Note 56**

5a0539b7021242e2a9a5769a1c156889

Let  $G$  a group,  $x \in G$ ,  $|x| = n < \infty$  and  $s \in \mathbb{Z}$ . Then

$$|x^s| = \frac{n}{(n, s)}.$$



### Note 57

7ec585d338e941d7b465cf11d0f42550

Let  $G$  a group,  $x \in G$ ,  $|x| = n < \infty$  and  $s \in \mathbb{Z}$ . Then  $|x^s| = \frac{n}{(n,s)}$ .  
What is the key idea in the proof?

■  $(x^s)^k = 1$  if and only if  $n \mid sk$ .

### Note 58

00c58492691e442b9a8c0a5ba21a0c7f

Let  $G$  a group,  $x \in G$ . If  $x^2 = 1$  then

$$x^{-1} = \langle\langle c1: x. \rangle\rangle$$

### Note 59

89199067c84244c094af347afff31c8a

Let  $G$  a group. If  $\langle\langle c3: a \text{ and } b \text{ are commuting elements of } G \rangle\rangle$  then  
 $\langle\langle c2: (ab)^n \rangle\rangle = \langle\langle c1: a^n b^n \rangle\rangle$ .

### Note 60

87374145922242e3a5bc43fa952448dc

Let  $G$  a group. If  $x^2 = 1$  for all  $x \in G$  then  $G$  is  $\langle\langle c1: \text{abelian.} \rangle\rangle$

### Note 61

cdf7b8b7731c4e619920d66f7520b423

Let  $G$  a group. If  $x^2 = 1$  for all  $x \in G$  then  $G$  is abelian. What is the key idea in the proof?

■  $1 = (ab)^2$  and multiply by  $a$  on the left and by  $b$  on the right.

### Note 62

c48695948e6a4cf69846a629c6b45cb5

Let  $(G, \star)$  be a group and  $\langle\langle c4: H \subseteq G. \rangle\rangle$  If  $\langle\langle c2: H \text{ is a group under the operation } \star \text{ restricted to } H \rangle\rangle$  then  $\langle\langle c3: H \rangle\rangle$  is called  $\langle\langle c1: \text{a subgroup of } G. \rangle\rangle$

### Note 63

7d6238e012914817a45ec81f6024cf10

Let  $(G, \star)$  and  $H \subseteq G$ . We shall say  $\langle\langle c2: H \text{ is closed under inverses} \rangle\rangle$  if  $\langle\langle c1: \text{for all } h \in H \text{ we have } h^{-1} \in H. \rangle\rangle$

### Note 64

b7191557c1c0477ba2b75dfd1485197d

Let  $(G, \star)$  be a group and  $H \subseteq G$  be nonempty. If  $H$  is closed under  $\star$  and inverses, then  $H$  is a subgroup of  $G$ .

### Note 65

39703ef9887d48e9b763bea0c6519b19

Let  $G$  a group and  $x \in G$ . Then the subgroup  $\{x^n \mid n \in \mathbb{Z}\}$  of  $G$  is called the cyclic subgroup of  $G$  generated by  $x$ .

### Note 66

7d1e317bc7c64c538d09a6fd6c2e2011

Let  $A$  and  $B$  be groups. Then  $A \times B$  is abelian if and only if both  $A$  and  $B$  are abelian.

### Note 67

c048d6c9ce83411c94e040e5991b3524

Let  $A$  and  $B$  be groups,  $(a, b) \in A \times B$ . Then the order of  $(a, b)$  is the least common multiple of  $|a|$  and  $|b|$ .

### Note 68

de71dcf7adc64bcd9b53502c90a0cefa

Let  $A$  and  $B$  be groups,  $(a, b) \in A \times B$ . Then

$$(a, b)^k = (a^k, b^k)$$

for all  $k \in \mathbb{Z}$ .

### Note 69

e672cc6907124507a4fd998675844d02

Let  $A$  and  $B$  be groups,  $(a, b) \in A \times B$ . Then the order of  $(a, b)$  is the least common multiple of  $|a|$  and  $|b|$ . What is the key idea in the proof?

■  $(a, b)^k = (a^k, b^k).$

### Note 70

c6f9e981e45d4f55a3aafa3eb6d77ef1

Any finite group of even order contains an element of order 2.

### Note 71

d13862b410194166829309d8ea4880a6

Any finite group of even order contains an element of order 2.  
What is the key idea in the proof?

■ Show that the set  $\{g \in G \mid g \neq g^{-1}\}$  has an even number of elements.

### Note 72

86e37f9ff199460995332631a61f9a00

Let  $G$  a group,  $x \in G$  and  $|x| = n < \infty$ . Then the elements

$$1, x, x^2, \dots, x^{n-1}$$

are distinct.

### Note 73

1bf4e9f92f854544bf96f1364e0064ed

Let  $G$  a group,  $x \in G$  and  $|x| < \infty$ . Then  $|x| \leq |G|$ .

### Note 74

5f4f77e21f2b4052979906547275dfd9

Let  $G$  a group,  $x \in G$  and  $|x| < \infty$ . Then  $|x| \leq |G|$ . What is the key idea in the proof?

■ The elements  $1, x, \dots, x^{n-1}$  are the only powers of  $x$ .

### Note 75

4f07acc87f6949e092c057cb5a580c77

Let  $G$  a group,  $x \in G$  and  $|x| = \infty$ . Then the elements

$$x^n, n \in \mathbb{Z}$$

are distinct.

# Dihedral Groups

## Note 1

c895ff9d20ae4a2286bb783680b3cee8

A symmetry of a regular  $n$ -gon is any rigid motion of the  $n$ -gon which can be effected by taking a copy of the  $n$ -gon, moving this copy in any fashion in 3-space and then placing the copy back on the original  $n$ -gon so it exactly covers it.

## Note 2

3a08bb223d9241bbb5cd4dae15a4a23d

Each symmetry of a regular  $n$ -gon can be described uniquely by the corresponding permutation of  $\{1, 2, \dots, n\}$ , representing the permutation of the vertices.

## Note 3

c0d6e6d3d60b45058b7957002e045102

Given  $n \in \mathbb{Z}^+$  and  $n \geq 3$ , the group of symmetries of a regular  $n$ -gon is called the dihedral group of order  $2n$ .

## Note 4

7a77331a22e144ceaf6ca7c1b475a99a

Given  $n \in \mathbb{Z}^+$  and  $n \geq 3$ , the dihedral group of order  $2n$  is denoted  $D_{2n}$ .

## Note 5

a81873dbe4e6432f93bb1d8c3c5978f1

Given  $n \in \mathbb{Z}^+$ ,  $n \geq 3$  and  $s, t \in D_{2n}$ , the product  $st$  is defined to be the symmetry obtained by first applying  $t$  then  $s$  to the  $n$ -gon.

## Note 6

1457d2279c1d432a9d371d8797d9b621

Given  $n \in \mathbb{Z}^+$  and  $n \geq 3$ ,

$$|D_{2n}| = 2n.$$

### Note 7

af77787eb9d94bae94d7df59b0415212

Given  $n \in \mathbb{Z}^+$  and  $n \geq 3$ ,  $|D_{2n}| = 2n$ . What is the key idea in the proof?

Every symmetry is uniquely determined by how it affects some two adjacent vertices.

### Note 8

1a3443407b8641c5adc691e47eef2f1e

For convenience, the regular  $n$ -gon viewed in  $D_{2n}$  is fixed centered at the origin.

### Note 9

b85d695a3fff47fba9b07b7a341cd0

For convenience, the vertices of the regular  $n$ -gon viewed in  $D_{2n}$  are labeled consecutively from 1 to  $n$  in a clockwise manner.

### Note 10

8005824717e34f4a8e154dfa84d25f17

In the context of the  $D_{2n}$  group, let  $r$  be the rotation clockwise about the origin through  $2\pi/n$  radian.

### Note 11

8439aae412044be9bf8f6c59334cd570

In the context of the  $D_{2n}$  group, let  $s$  be the reflection about the line of symmetry through vertex 1 and the origin.

### Note 12

d46303ae65e74f2e8f610b873f4e559b

In the context of the  $D_{2n}$  group, is it possible that  $s = r^i$  for some  $i$ ?

No.

### Note 13

5aaf131bef484c89b455ce9f5b4a2eae

In the context of the  $D_{2n}$  group, is it possible that  $sr^i = sr^j$  for some  $i \not\equiv j \pmod{n}$ ?

■ No.

### Note 14

79c14b3dba52416f934c9d820acb0be7

Each element of  $D_{2n}$  can be written uniquely in the form  $s^k r^i$  for some  $k = 0$  or  $1$  and  $0 \leq i \leq n - 1$ .

### Note 15

f3a7147f62d84c53b1ecc4f7da081eba

In the context of the  $D_{2n}$  group,

$$r^i s = sr^{-i}, \text{ for all } 0 \leq i \leq n.$$

### Note 16

2600f25fd1ec408b8e47e341dc6cdb64

In the context of the  $D_{2n}$  group,

$$r^i s = sr^{-i}, \text{ for all } 0 \leq i \leq n.$$

What is the key idea in the proof?

■  $rs = sr^{-1}$  and by induction.

### Note 17

f56559b6eae841cea409f8438221c1b2

A subset  $S$  of elements of a group  $G$  with the property that every element of  $G$  can be written as a (finite) product of elements of  $S$  and their inverses is called a set of generators of  $G$ .

### Note 18

d72e348121f94214980378f08a5e45a3

If  $S$  is a set of generators of a group  $G$ , we shall write

$$G = \langle S \rangle.$$

}}

### Note 19

7bc8f288fd5d45e0a89eb59abdc95810

If  $S$  is a set of generators of a group  $G$ , we shall say  $G$  is generated by  $S$ .

## Note 20

cb072c7b416e4fbf8e3cf95f496f4083

In terms of generators, the group  $D_{2n} = \langle r, s \rangle$ .

## Note 21

4fd6980a252a486980db01306accceef

In a finite group  $G$  a set  $S$  generates  $G$  if every element of  $G$  is a finite product of elements of  $S$ .

## Note 22

90b6154b7aaa48398ddecb91083d71ac

In the  $D_{2n}$  group, the relations  $r^n = 1$ ,  $s^2 = 1$  and  $rs = sr^{-1}$  have the additional property that any other relation between elements of the group may be derived from these three.

## Note 23

4681975ee07c4032a3ced2de0ccfa631

In the  $D_{2n}$  group, the relations  $r^n = 1$ ,  $s^2 = 1$  and  $rs = sr^{-1}$  have the additional property that any other relation between elements of the group may be derived from these three. What is the key idea in the proof?

We can determine exactly when two group elements are equal by using only these three relations.

## Note 24

b0bcc70704c64eccba8d832a4540749b

Let  $G$  be a group. Any equations in  $G$  that the generators satisfy are called relations in  $G$ .

## Note 25

b8f9a5669c634d39ac14a6115f6b142d

Let  $G$  be a group. If  $G$  is generated by a subset  $S$  and there is some collection of relations such that any relation among the elements of  $S$  can be deduced from these, we shall call these generators and relations a presentation of  $G$ .

## Note 26

265ab5c6f292430c8ecc6ab97f25c8a8

Let  $G$  be a group. If  $\langle S \rangle$  is a subset  $S$  and  $\{R_1, \dots, R_m\}$  a collection of relations  $R_1, \dots, R_m$  form a presentation of  $G$ , we shall write

$$G = \langle S \mid R_1, \dots, R_m \rangle.$$

}

## Note 27

b8acfa74c7df4502a3b76c59342afbac

One presentation of the dihedral group  $D_{2n}$  is

$$\langle D_{2n} \rangle = \langle r, s \mid r^n = s^2 = 1, rs = sr^{-1} \rangle.$$

## Note 28

06f27cb1fae140be909a72d4d52162a8

If  $n = 2k$  is even and  $n \geq 4$  then  $\langle r^k \rangle$  is the only nonidentity element of  $D_{2n}$  which commutes with all elements of  $D_{2n}$ .



# Symmetric Groups

## Note 1

35103f7401374322997a41574a878c47

Given a set  $\Omega$ , the set of all bijections from  $\Omega$  to itself is denoted  $S_\Omega$ .

## Note 2

e190a5ea3cc542a09f5d22434fd383e7

Let  $\Omega$  be a nonempty set. Then the group  $(S_\Omega, \circ)$  is called the symmetric group on the set  $\Omega$ .

## Note 3

41b5292492ba47c2b0c6733f4d86e86e

Let  $n \in \mathbb{Z}^+$ . The symmetric group on the set  $\{1, 2, \dots, n\}$  is called the symmetric group of degree  $n$ .

## Note 4

b7fae74ed3df4e71b785bd65d2e5e42b

Let  $n \in \mathbb{Z}^+$ . The symmetric group of degree  $n$  is denoted  $S_n$ .

## Note 5

40a80f61353b460c9200ea835050fc6d

Let  $n \in \mathbb{Z}^+$ . Then

$$|S_n| = n!$$

## Note 6

971a7ee9395248c3ad6b53fc7e57223c

A cycle is a string of integers which represents the element of  $S_n$  which cyclically permutes these integers (and fixes all other integers).

## Note 7

0d979e8f5d444cd2b20479e738e3b244

The cycle  $(a_1 \ a_2 \ \dots \ a_m)$  in  $S_n$  is the permutation

$$a_i \mapsto a_{i+1} \quad a_m \mapsto a_1.$$

}

### Note 8

1ecd3b35c9e34999a9cd7481ad891e0d

The length of a cycle in  $S_n$  is the number of integers that appear in it.

### Note 9

d53a85a6dc624da7b74414131a5c9b0b

A cycle of length  $t$  in  $S_n$  is called a  $t$ -cycle.

### Note 10

69e31cdb5b8644e790c3368b3b37f9fc

Two cycles in  $S_n$  are called disjoint if they have no numbers in common.

### Note 11

d1990b072a9244dca0f3ae3ea60a5bf0

Let  $\sigma \in S_n$ . The representation of  $\sigma$  as the products of pairwise disjoint cycles is called the cycle decomposition of  $\sigma$ .

### Note 12

562293a2603f483ab79fd4e9cbd6d36e

The identity permutation of  $S_n$  will be written as  $1$ .

### Note 13

2e6d113b0fdf478f9cacb6d733a989c3

$S_n$  is a non-abelian group for all  $n \geq 3$ .

### Note 14

3ff49b43f20f4b3390f3e555c41492a1

Disjoint cycles in  $S_n$  commute.

### Note 15

6c2a6cc5ad27457db08cdcca242f5353

The cycle decomposition of each permutation in  $S_n$  is the unique way of expressing a permutation as a product of disjoint cycles (up to rearrangement).

### Note 16

f1f1d98922ba4affa25f8a1500989973

The order of a permutation in  $S_n$  is the l.c.m. of the lengths of the cycles in its cycle decomposition.

### Note 17

e539f64a563146f68a90f700cee3c2a6

Let  $\sigma$  be a  $k$ -cycle in  $S_n$ . Then

$$|\sigma| = \{\{c1: k.\}\}$$

### Note 18

0f104518132a45bf947b3861439a4677

Let  $\sigma$  be a  $k$ -cycle in  $S_n$ . For which positive integers  $i$  is  $\sigma^i$  also a  $k$ -cycle?

■ For  $i$  relatively prime to  $k$ .

### Note 19

2c81a75df4394dd8945d760a2dd538a3

Let  $\sigma$  be a  $k$ -cycle in  $S_n$ . What is special about the cyclic decomposition of  $\sigma^i$  for an arbitrary  $i \in \mathbb{Z}^+$ ?

■ All of the disjoint cycles have the same length and are “evenly spaced.”

### Note 20

a6f4e4da4d104be3b33ee481ae4a34fc

Let  $p$  be  $\{\{c3: \text{a prime.}\}\}$ . An element has order  $\{\{c2: p\}\}$  in  $S_n$  if and only if  $\{\{c4: \text{its cycle decomposition}\}\}$  is  $\{\{c1: \text{a product of commuting } p\text{-cycles.}\}\}$

### Note 21

1cebfe78ebcb423e82d93932c114de3b

$$\{\{c4: S_3\}\} = \langle a, b \mid \{\{c1: a^2 = b^2 = 1, \}\} \{\{c2: aba = bab\}\} \rangle,$$

where  $a = \{\{c3: (1\ 2)\}\}$ ,  $b = \{\{c3: (2\ 3)\}\}$ .

# Matrix Groups

## Note 1

d24745203ab949c39f465e4e32838554

First, a field is  $\{\{c2::a \text{ set } F\}\}$  together with  $\{\{c1::\text{two binary operations } + \text{ and } \cdot \text{ on } F.\}\}$

## Note 2

f3c03aa477f94f80bb772b9ea31136f9

How are the properties of  $+$  summarised in the definition of a field  $F$ ?

■  $(F, +)$  is an abelian group.

## Note 3

dace43278a624b1a8496c81bfef9be5b

How are the properties of  $\cdot$  summarised in the definition of a field  $F$ ?

■  $(F - \{0\}, \cdot)$  is an abelian group.

## Note 4

bc1d11a398434735a6129ece90078d0b

In the definition of a field  $F$ , what does  $0$  refer to?

■ The identity of  $F$  with respect to  $+$ .

## Note 5

a12c4072b03f4f4385856eb63232dc6e

What is the key property that relates  $+$  and  $\cdot$  in the definition of a field  $F$ ?

■ The distributive law.

## Note 6

e20af7d49d0f467694122bf0aad50c59

The distributive law from the definition of a field  $F$  states that

$\{\{c1::$

$$a \cdot (b + c) = (a \cdot b) + (a \cdot c), \quad \text{for all } a, b, c \in F.$$

$\}\}$

## Note 7

34af1e3acbf4b2e8485bd9ddf265c4a

For any field  $F$  let  $\{\{c2::F^\times\}\} = \{\{c1::F - \{0\}\}\}$ .

## Note 8

18535f79dcff4a67b32868a9f60b8f7e

Given  $\{\{c3::\text{a prime } p,\}\}$  we shall denote  $\{\{c1::\text{the field } \mathbb{Z}/p\mathbb{Z}\}\}$  as  $\{\{c2::\mathbb{F}_p\}\}$  to emphasize that  $\{\{c4::\text{it is a field.}\}\}$

## Note 9

53ab9021abdc4aab9077b752f52df492

Given  $\{\{c3::n \in \mathbb{Z}^+\}\}$  and  $\{\{c4::\text{a field } F,\}\}$   $\{\{c1::\text{the general linear group of degree } n\}\}$  is denoted  $\{\{c2::$

$$GL_n(F).$$

$\}\}$

## Note 10

26483d8a0f29448db95af373c3315d8f

What are the elements of  $GL_n(F)$ ?

■ All  $n \times n$  matrices whose entries come from a field  $F$  and whose determinant is nonzero.

## Note 11

62ca6e7bafed4c0fa4621e7fcb7a612d

What is the operation of  $GL_n(F)$ ?

■ Matrix multiplication.

## Note 12

ecd39cec434e4ca58d71efd99f59f652

Let  $F$  be a field. If  $\{\{c2::|F| < \infty,\}\}$  then

$$\{\{c3::|F|\}\} = \{\{c1::p^m \text{ for some prime } p \text{ and an integer } m.\}\}$$

## Note 13

4262c7c840fb4996904e2a18838f8766

Let  $F$  be a field. If  $\{\{c4::|F| = q < \infty,\}\}$  then

$$\{\{c3::|GL_n(F)|\}\} = \prod_{k=\{\{c2::0\}\}}^{\{\{c2::n-1\}\}} \{\{c1::(q^n - q^k).\}\}$$

### Note 14

81873bd4066c43069f33d507d19a4f29

Let  $F$  be a field. The subgroup of all the unit upper triangular matrices in  $GL_3(F)$  is called the Heisenberg group over  $F$ .

### Note 15

ab984848eb1941a4ba184e6bc8efece7

Let  $F$  be a field. The Heisenberg group over  $F$  is denoted  $H(F)$ .

### Note 16

dfc23a9c6de94344a15a98b09a255950

Let  $F$  be a field. Then

$$|H(F)| = |F|^3.$$

### Note 17

d23fde00126540ae999cadfb9f0101f4

Let  $x \in H(\mathbb{R})$ . If  $x \neq 1$ , then

$$|x| = \infty.$$

# The Quaternion Group

## Note 1

239ae951128a45148a7a0b069837604e

The quaternion group is denoted  $Q_8$ .

## Note 2

555bc9c4e6e549a8954f57e369620c61

$$Q_8 = \{1, -1, i, -i, j, -j, k, -k\}.$$

## Note 3

6e7c0944844b48afb9531e5d1fa28c7

$$|Q_8| = 8.$$

## Note 4

4227539ce42c4875a7adfb3ca6f82b3

In  $Q_8$ ,  $1 \cdot x = x \cdot 1 = x$ , for all  $x$ .

## Note 5

fe801d8cadf94adc8af7a8f10209ed3b

In  $Q_8$ ,  $(-1) \cdot x = x \cdot (-1) = -x$ , for all  $x$ .

## Note 6

3b0e08d205ac4eb59c5eb69b79b45201

In  $Q_8$ ,  $(-1) \cdot (-1) = 1$ .

## Note 7

c779211682144018898526c5025c9048

In  $Q_8$ ,  $i \cdot i = -1$ .

## Note 8

796029c2d52b43d6944db20f10fdd8af

In  $Q_8$ ,  $j \cdot j = -1$ .

## Note 9

ec5bd7ed074a42d6ba94f6bd9da19392

In  $Q_8$ ,  $k \cdot k = -1$ .

## Note 10

e38c1bab9ae74d96b1ad4505d46d0417

In  $Q_8$ ,  $i \cdot j = k$ .

**Note 11**

15482b24d8c34da580643a244f8080dc

$$\text{In } Q_8, \quad j \cdot k = \langle\langle c1::i \rangle\rangle.$$

**Note 12**

654c41a13a224d9f941e791b4ce340e1

$$\text{In } Q_8, \quad k \cdot i = \langle\langle c1::j \rangle\rangle.$$

**Note 13**

9be42c8a75764261a0ec49fd8d867350

$$\text{In } Q_8, \quad j \cdot i = \langle\langle c1:: -k \rangle\rangle.$$

**Note 14**

de5cd3f588fd4c59a098434677b65581

$$\text{In } Q_8, \quad k \cdot j = \langle\langle c1:: -i \rangle\rangle.$$

**Note 15**

b0e3385e5ab240d88ab165e2347bedc9

$$\text{In } Q_8, \quad i \cdot k = \langle\langle c1:: -j \rangle\rangle.$$

**Note 16**

34b82771d5ed4619b3024d89b76ed248

$$Q_8 = \langle\langle\langle c1::i, j \rangle\rangle\rangle$$

**Note 17**

e8cdf713f64b4e39b536f9b52b4ee716

$$\langle\langle c3::Q_8 \rangle\rangle = \langle i, j \mid \langle\langle c1::i^2 = j^2, \rangle\rangle \langle\langle c2::ij = ji^{-1} \rangle\rangle \rangle.$$



# Homomorphisms and Isomorphism

## Note 1

96860b79fbf04dc09da2c397394f3238

Let  $(G, \star)$  and  $(H, \diamond)$  be groups. A map  $\varphi : G \rightarrow H$  such that

$$\varphi(x \star y) = \varphi(x) \diamond \varphi(y), \quad \text{for all } x, y \in G$$

is called a homomorphism.

## Note 2

e30cd56ca334447195645d566046ce38

Let  $G$  and  $H$  be groups. A map  $\varphi : G \rightarrow H$  is called an isomorphism if it is a bijective homomorphism.

## Note 3

b2c556679c0e45a6b32ec8e8790a54c0

Let  $G$  and  $H$  be groups.  $G$  and  $H$  are said to be isomorphic or of the same isomorphism type if there exists an isomorphism  $G \rightarrow H$ .

## Note 4

1a95e054ea864182b2ea76e195bb7481

Let  $G$  and  $H$  be groups. If  $G$  and  $H$  are isomorphic we shall write

$$G \cong H.$$

}

## Note 5

1cd3c49fc5504bbeb32520664e32242d

Let  $\mathcal{G}$  be a nonempty collection of groups. Then  $\cong$  is an equivalence relation on  $\mathcal{G}$ .

## Note 6

ee4d500cb1d74f94967ba13f8ba4504a

Let  $\mathcal{G}$  be a nonempty collection of groups. The equivalence classes of  $\cong$  are called isomorphism classes.

## Note 7

284b06e23e8a4abba099fb983d10b5a1

The map  $x \mapsto e^x$  is an isomorphism from  $(\mathbb{R}, +)$  to  $(\mathbb{R}^+, \times)$ .

## Note 8

f462694f01354b2dbe42e428795fe196

The isomorphism type of a symmetric group depends **only** on the cardinality of the underlying set being permuted.

## Note 9

270ed61fd46c4d37815329b5c32c58cd

Let  $\Delta$  and  $\Omega$  be nonempty sets. Then  $S_\Delta \cong S_\Omega$  if and only if

$$|\Delta| = |\Omega|.$$

}}

## Note 10

83592018138d4e7aa463202f134641aa

Let  $\Delta$  and  $\Omega$  be nonempty sets. Then  $S_\Delta \cong S_\Omega$  if  $|\Delta| = |\Omega|$ . What is the key idea in the proof?

■ Build an isomorphism using a bijection  $\Delta \rightarrow \Omega$ .

## Note 11

412d560d91f1457582455d66f228bfb4

Let  $\Delta$  and  $\Omega$  be nonempty sets. Then  $S_\Delta \cong S_\Omega$  if  $|\Delta| = |\Omega|$ . In the proof, how do we define the isomorphism  $\varphi$ ?

■  $\varphi(\sigma) = \theta \circ \sigma \circ \theta^{-1}$ , where  $\theta : \Delta \rightarrow \Omega$  is a bijection.

## Note 12

5fea8ecc491b4cdc9c34f69f48157b76

Theorems that determine what properties of a structure specify its isomorphism type are referred to as **classification theorems**.

}}

## Note 13

9b1e1641c6d64bb6af49a60adc2cc8aa

If  $\varphi : G \rightarrow H$  is a group isomorphism, then

$$|G| = |H|.$$

**Note 14**

3c156770eb5c46be965e82efae228841

If  $\varphi : G \rightarrow H$  is a group isomorphism, then

$$H \text{ is abelian } \Leftrightarrow G \text{ is abelian.}$$

**Note 15**

b2ede5339fce42f3abd2efb2ddce810f

If  $\varphi : G \rightarrow H$  is a group isomorphism and  $x \in G$ , then

$$|\varphi(x)| = |x|.$$

**Note 16**

419a5ad390f344458c0e7691b738bc35

Let  $G$  and  $H$  be groups,  $|G| < \infty$  and

$$G = \langle s_1, \dots, s_m \mid R_1, \dots, R_k \rangle, \\ \{r_1, \dots, r_m\} \subseteq H.$$

If any relation  $R_j$  is satisfied in  $H$  when each  $s_i$  is replaced by  $r_i$ , then there is a unique homomorphism

$$\varphi : G \rightarrow H, \quad s_i \mapsto r_i.$$

}}

**Note 17**

01c1c1207426404aa19d1999da72740e

Let  $G$  and  $H$  be groups,  $|G| < \infty$ , and

$$G = \langle s_1, \dots, s_m \mid R_1, \dots, R_k \rangle, \\ \{r_1, \dots, r_m\} \subseteq H,$$

$\varphi : s_i \mapsto r_i$  be a homomorphism.

If  $H$  is generated by  $\{r_1, \dots, r_m\}$ , then  $\varphi$  is surjective.

**Note 18**

8f56d68fe62346659ff46ae2b1f31651

Let  $G$  and  $H$  be groups,  $|G| < \infty$ , and

$$G = \langle s_1, \dots, s_m \mid R_1, \dots, R_k \rangle,$$

$$\{r_1, \dots, r_m\} \subseteq H,$$

$\varphi : s_i \mapsto r_i$  be a homomorphism.

If  $\{\{c3::H \text{ is generated by } \{r_1, \dots, r_m\}\}\}$  and  $\{\{c2::|H| = |G|,\}\}$  then  $\{\{c1::\varphi \text{ is an isomorphism.}\}\}$

**Note 19**

67b60cd5209c46fbbb3f98e3f10b05e1

$$D_{\{\{c2::6\}\}} \cong S_{\{\{c1::3\}\}}.$$

**Note 20**

1f9aa544bf9a4eb4a414531f8156f4cd

$D_6 \cong S_3$ . What is the key idea in the proof?

■ Build a homomorphism using the presentation of  $D_6$ .

**Note 21**

a042a5ebe7b449ff86ce5a24db9bb191

$D_6 \cong S_3$ . Which generator of  $D_6$  are used in the proof?

■  $r$  and  $s$ .

**Note 22**

1daa5ca4598f44fcbd36ec24a840501e

$D_6 \cong S_3$ . Which generator of  $S_3$  are used in the proof?

■  $a = (1\ 2)$  and  $b = (1\ 2\ 3)$ .

**Note 23**

d9a1d23815594891aa15dd743f29acfc

Let  $\varphi : G \rightarrow H$  be a group homomorphism. Then

$$\varphi(x^n) = \{\{c1::\varphi(x)^n\}\} \quad \text{for all } n \in \{\{c2::\mathbb{Z},\}\}$$

**Note 24**

2ac7af235abd475ea3f54b2b250b4400

Let  $\varphi : G \rightarrow H$  be a group homomorphism. Then

$$\varphi(x^{-1}) = \{\{c1::\varphi(x)^{-1},.\}\}$$

**Note 25**

2dc3b42cb1a242a49fce2ea25c98de72

Let  $\varphi : G \rightarrow H$  be a group homomorphism. Then

$$\varphi(1) = \{\{c1::1,.\}\}$$

**Note 26**

71cc11a4e7454bd4ab3e4eebc22c9eb1

Let  $\varphi : G \rightarrow H$  be a group  $\{\{c3::\text{isomorphism},.\}\}$  Then

$$\varphi(x) = 1_{\{\{c2::\}} \iff \}\{\{c1::x = 1,.\}\}$$

**Note 27**

f48d2a825d984e4b823201c3b6b9d3de

Let  $\varphi : G \rightarrow H$  be a group homomorphism. Is it unconditionally true that  $|\varphi(x)| = |x|$  for all  $x \in G$ ?

■ No.

**Note 28**

844e79dfacbc4157acfd4aebdbaa4947

Let  $\varphi : G \rightarrow H$  be a group homomorphism and  $G$  be abelian. Then

$$\{\{c1::\varphi \text{ is surjective},.\}\} \{\{c3::\} \implies \}\{\{c2::H \text{ is abelian},.\}\}$$

**Note 29**

aec0f7a10a044411b844a5a08d3303d9

Are the groups  $(\mathbb{R}, +)$  and  $(\mathbb{R}^+, \times)$  isomorphic?

■ Yes.

### Note 30

57b13746efbe42fda870594eda8f6965

Are  $D_6$  and  $S_3$  isomorphic?

■ Yes.

### Note 31

4a3c6aee4f084dfea611c081da1c5925

Are the multiplicative groups  $\mathbb{R}^\times$  and  $\mathbb{C}^\times$  isomorphic?

■ No.

### Note 32

b33c67212d1444d3a8679e7c31a39c66

The multiplicative groups  $\mathbb{R}^\times$  and  $\mathbb{C}^\times$  are not isomorphic. What is the key idea in the proof?

■  $\mathbb{C}^\times$  has elements of order  $n > 2$ .

### Note 33

ded0e803e7e34c5f913f8a715f6186b0

Are the additive groups  $\mathbb{R}$  and  $\mathbb{Q}$  isomorphic?

■ No.

### Note 34

e7bf7586388f460993d9976f09ab36d5

The additive groups  $\mathbb{R}$  and  $\mathbb{Q}$  are not isomorphic. What is the key idea in the proof?

■  $|\mathbb{R}| \neq |\mathbb{Q}|$ .

### Note 35

5de7b924c5d74c24bebd18083881ebd6

Are the additive groups  $\mathbb{Z}$  and  $\mathbb{Q}$  isomorphic?

■ No.

### Note 36

033cd7915d6349bead591259dd238b2d

The additive groups  $\mathbb{Z}$  and  $\mathbb{Q}$  are not isomorphic. What is the key idea in the proof?

■  $\mathbb{Q}$  has elements of order  $n > 1$ .

### Note 37

42380e58738b40099ecc62e995bc6049

Are  $D_8$  and  $Q_8$  isomorphic?

■ No.

### Note 38

c920ffc0d7ba4faeb1cfc6748bbb0df5

$D_8$  and  $Q_8$  are not isomorphic. What is the key idea in the proof?

■  $D_8$  has for elements of order 2, namely  $s, sr, sr^2, sr^3$ .

### Note 39

7f2f3fa158c7439f8857975eadb00fc5

Are  $D_{24}$  and  $S_4$  isomorphic?

■ No.

### Note 40

e883c893667e4f09b6f83f082c41281a

$D_{24}$  and  $S_4$  are not isomorphic. What is the key idea in the proof?

■  $D_{24}$  has an element of order 12.

### Note 41

d5bb3b5b1d3c440caaeab945defc239d

Let  $A$  and  $B$  be groups. Are  $A \times B$  and  $B \times A$  isomorphic?

■ Yes.

### Note 42

c47557cf76554d059f5755de18a4df00

Let  $A$ ,  $B$  and  $C$  be groups. Are  $(A \times B) \times C$  and  $A \times (B \times C)$  isomorphic?

■ Yes.

### Note 43

0e9033cc45ee4e97917feb313e9598ac

Let  $\varphi : G \rightarrow H$  be a group homomorphism. Then  $\{\{c3:: \text{the image}\}$  of  $\varphi$  is  $\{\{c1:: \text{a subgroup}\}$  of  $\{\{c2:: H.\}\}$

### Note 44

2771feb8afd448049fd587b560e40ec9

Let  $\varphi : G \rightarrow H$  be a group homomorphism. Then

$$\{\{c2:: \varphi \text{ is injective}\}\}\{\{c5:: \iff\}\}\{\{c3:: G\}\}\{\{c4:: \cong\}\}\{\{c1:: \varphi(G).\}\}$$

### Note 45

12077d31c47349a5bceacda0fde9ea1

Let  $\varphi : G \rightarrow H$  be a group homomorphism. If  $\varphi$  is injective then  $G \cong \varphi(G)$ . What is the key idea in the proof?

■  $\varphi$  is surjective when its codomain is restricted to  $\varphi(G)$ .

### Note 46

2a8327bf4f684de0b39f3817aad067b9

Let  $\varphi : G \rightarrow H$  be a group homomorphism.  $\{\{c2:: \text{The kernel of } \varphi\}$  is  $\{\{c1:: \text{the fiber of } \varphi \text{ over } 1.\}\}$

### Note 47

b3a98b9d64f74a20acda1441ecdc9369

Let  $\varphi : G \rightarrow H$  be a group homomorphism. Then  $\{\{c3:: \text{the kernel}\}$  of  $\varphi$  is  $\{\{c1:: \text{a subgroup}\}$  of  $\{\{c2:: G.\}\}$

### Note 48

f41a2cf31300472c964735adcca416bd

Let  $\varphi : G \rightarrow H$  be a group homomorphism. Then  $\{\{c3:: \varphi \text{ is injective}\}$   $\{\{c4:: \text{if and only if}\}\}$   $\{\{c2:: \text{the kernel of } \varphi\}\}$   $\{\{c1:: \text{is the identity subgroup of } G.\}\}$



**Note 49**

086cd029adec4c3185796e6c095f117c

Let  $G$  be a group. Then the map  $g \mapsto g^{-1}$  is a homomorphism  
 if and only if  $G$  is abelian.

**Note 50**

f748fe4d306c4cfe8ab2701c9737cac4

Let  $G$  be a group. Then the map  $g \mapsto g^2$  is a homomorphism  
 if and only if  $G$  is abelian.

**Note 51**

a34cd518f90a4b80aa8fa09ec58f79b5

Is any surjective homomorphism necessarily an isomorphism?

■ No.

**Note 52**

be5f48d2e20e41dbbab81bc5b7d6334c

Let  $G$  be a group. An isomorphism from  $G$  onto  $G$  is called  
 an automorphism of  $G$ .

**Note 53**

175a31f669ee492bb4698ccb5a311115

Let  $G$  be a group. The set of all automorphisms of  $G$  is denoted

$$\text{Aut}(G).$$

}

**Note 54**

bf4133e84db44fd4a19013814259b4f1

Let  $G$  be a group. Then  $\text{Aut}(G)$  is a group under function  
 composition.

**Note 55**

3d4887e6cf02407b97125275d1ae4b0b

Let  $G$  be a group. The group  $(\text{Aut}(G), \circ)$  is called the  
 automorphism group of  $G$ .

**Note 56**

29c4a6993b1c42d9b60563794a41dd58

Let  $G$  be a group. A homomorphism  $\sigma$  such that

$$\sigma(g) = g \text{ implies } g = 1$$

is called fixed point free.

### Note 57

10d4efc454cd45189f531b1b8e225ebf

Let  $G$  be a finite group. If  $\sigma$  is a fixed point free automorphism of order 2 in  $G$ , then

$$\sigma : x \mapsto x^{-1}.$$

### Note 58

48b10b987faa4173afd091d11bce69f8

Let  $G$  be a finite group. If  $\sigma$  is a fixed point free automorphism of order 2 in  $G$ , then  $\sigma : x \mapsto x^{-1}$ . What is the key idea in the proof?

Any  $x \in G$  may be expressed as  $g^{-1}\sigma(g)$  for some  $g \in G$ .

### Note 59

559ae14dc2c142eba35c1b72238ad25e

Let  $G$  be a finite group. If  $G$  possesses a fixed point free automorphism of order 2, then  $G$  is abelian.

### Note 60

47792a9d48b64045b05ea3dd789e8d12

Let  $G$  be a finite group. If  $G$  possesses a fixed point free automorphism of order 2, then  $G$  is abelian. What is the key idea in the proof?

The automorphism must be  $x \mapsto x^{-1}$ .

### Note 61

ee7230fadcc9450e89d741cb94e940d7

Let  $G = \langle x, y \rangle$  be a finite group,  $x \neq y$  and  $|x| = |y| = 2$ . Then

$$G \cong D_{2n},$$

where  $n = |xy|$ .

# Group Actions

## Note 1

47fb1f971a0e47ca900bca9d515b276f

Let  $G$  be a group and  $A$  be a set. First, a group action of  $G$  on  $A$  is a map from  $G \times A$  to  $A$ .

## Note 2

0949588890c9477795b23452373695d9

Let  $G$  be a group and  $A$  be a set. The group action of  $G$  on  $A$  is written

$$(g, a) \mapsto g \cdot a.$$

## Note 3

9f314e8d6fb04ba78bda7bde0c259aa5

Let  $G$  be a group and  $A$  be a set. How many properties are there in the definition of a group action of  $G$  on  $A$ ?

■ Two.

## Note 4

2150fd542e2b4a4483ef8f54aafebf19

Let  $G$  be a group and  $A$  be a set. What is the first property from the definition of a group action of  $G$  on  $A$ ?

■  $g \cdot (h \cdot a) = (gh) \cdot a$  for all  $g, h \in G, a \in A$ .

## Note 5

c886b7ab9579413389c0a1a864a71f9b

Let  $G$  be a group and  $A$  be a set. What is the second property from the definition of a group action of  $G$  on  $A$ ?

■  $1 \cdot a = a$  for all  $a \in A$ .

## Note 6

923e161350c04b37925f4d8a5ec7a48f

Let  $G$  be a group. We shall say  $G$  acts on a set  $A$  if a group action of  $G$  on  $A$  is given.

### Note 7

4a108c989e364bf1a4f08acf4b13afed

Let a group  $G$  act on a set  $A$ . Given  $g \in G$  and  $a \in A$ , the expression  $\{\{c2::g \cdot a\}\}$  will usually be written  $\{\{c1::\text{simply as } ga.\}\}$

### Note 8

1e4797055dac4aaebaff4f3e7ca94dc9

Let a group  $G$  act on a set  $A$ . Given  $\{\{c4::g \in G,\}\}$  the map  $\{\{c3::\sigma_g\}\}$  is defined by

$$\{\{c3::\sigma_g\}\} : \{\{c2::A\}\} \rightarrow \{\{c2::A\}\} \quad a \mapsto \{\{c1::g \cdot a.\}\}$$

### Note 9

a7a8a2e8422c4eb1a55326e03fdfac3e

Let a group  $G$  act on a set  $A$ . For each fixed  $g \in G$ ,  $\sigma_g$  is  $\{\{c1::\text{a permutation}\}\}$  of  $A$ .

### Note 10

069a58b690ce40bcb6ac7e8b2bd10732

Let a group  $G$  act on a set  $A$ . For each fixed  $g \in G$ ,  $\sigma_g$  is a permutation of  $A$ . What is the key idea in the proof?

■ Find the 2-sided inverse of  $\sigma$ .

### Note 11

3d3a86bc4244429da7757d00efca180a

Let a group  $G$  act on a set  $A$ . Given  $g \in G$ ,

$$\{\{c2::\sigma_g^{-1}\}\} = \{\{c1::\sigma_{g^{-1}}.\}\}$$

### Note 12

3c4e03fddab413f84ca6812e5ffed8e

Let a group  $G$  act on a set  $A$ . The map from  $G$  to  $\{\{c3::S_A\}\}$  defined by

$$g \mapsto \{\{c2::\sigma_g\}\}$$

is  $\{\{c1::\text{a homomorphism.}\}\}$

### Note 13

a3383f0de3ab4bb48b322d1900ca9519

Intuitively,  $\{\{c3:: \text{a group action of } G \text{ on a set } A\}\}$  just means that every element  $g$  in  $G$  acts as  $\{\{c1:: \text{a permutation}\}\}$  on  $A$  in a manner  $\{\{c2:: \text{consistent with the group operations in } G.\}\}$

### Note 14

2bd735bbaef44a68e6820678cdfd0ef

Let a group  $G$  act on a set  $A$ .  $\{\{c3:: \text{The homomorphism } g \mapsto \sigma_g\}\}$  from  $\{\{c4:: G\}\}$  to  $\{\{c4:: S_A\}\}$  is called  $\{\{c1:: \text{the permutation representation}\}\}$   $\{\{c2:: \text{associated to the given action.}\}\}$

### Note 15

c1df0995320a40d2a6d9ee88309ffada

Let  $G$  be a group and  $\{\{c5:: A \text{ a set.}\}\}$  Any  $\{\{c3:: \text{homomorphism}\}\}$   $\{\{c1::$

$$\varphi : G \rightarrow S_A$$

$\}\}$  corresponds to  $\{\{c2:: \text{a group action of } G \text{ on } A.\}\}$

### Note 16

b74b0d2663b04de589ca4386ed7cfef4

Let  $G$  be a group and  $A$  a set. To which group action does a homomorphism  $\varphi : G \rightarrow S_A$  correspond?

|

$$g \cdot a = \varphi(g)(a).$$

### Note 17

5974a55856e34f02b8ea7ea3aa308ede

Let  $G$  be a group. More precisely, a group action of the form  $\{\{c2::$

$$G \times A \rightarrow A$$

$\}\}$  should be named  $\{\{c1:: \text{a left action.}\}\}$

### Note 18

98196731647644bbb8b84f0dd0e9ba38

Let  $G$  be a group and  $A$  a nonempty set. The action of  $G$  on  $A$  defined by  $\{\{c1::$

$$ga = a, \quad \text{for all } g \in G, a \in A$$

$\}\}$  is called  $\{\{c2:: \text{the trivial action.}\}\}$

### Note 19

e3f75516876e4c8396233ef839dc2834

Let  $G$  be a group acting on a set  $A$ . We shall say  $\{\{c2::G \text{ acts trivially on } A\} \text{ if } \{\{c1:: \text{the action is trivial.}\}\}$

### Note 20

e845e29f5f0145adb058744cfa19d71a

Let  $G$  be a group acting on a set  $A$ . If  $\{\{c2:: \text{distinct elements of } G \text{ induce distinct permutations of } A,\} \}$  the action is said to be  $\{\{c1:: \text{faithful.}\}\}$

### Note 21

1d6ec9bd320440c7948bea6cc552bf8f

A group action  $\{\{c3:: \text{is faithful}\} \}$   $\{\{c4:: \text{if and only if}\} \}$   $\{\{c2:: \text{the associated permutation representation}\} \}$   $\{\{c1:: \text{is injective.}\}\}$

### Note 22

3b17f64aea804c2ca27b2bc733a2a014

Let  $G$  be a group acting on a set  $A$ .  $\{\{c2:: \text{The kernel of the action}\} \}$  is defined to be  $\{\{c1::$

$$\{g \in G \mid \sigma_g = 1\}.$$

$\}\}$

### Note 23

d3de7470fa0e4b758296c348c93d3fdf

Let  $V$  be a vector space over a field  $F$ . Then  $\{\{c2:: \text{the multiplicative group } F^\times \} \}$   $\{\{c3:: \text{acts}\} \}$  on  $\{\{c1:: \text{the set } V.\} \}$

### Note 24

6e14b840046548aa83a89f744766a642

For any nonempty set  $A$  the group  $S_A$  acts on  $A$  by  $\sigma \cdot a = \{\{c1:: \sigma(a)\}\}$ , for all  $\sigma \in S_A, a \in A$ .

### Note 25

2b11c4a7f35b44008803b61ae22c4ec1

Let  $A$  be a nonempty set. The permutation representation associated with the action of  $S_A$  on  $A$  is  $\{\{c1:: \text{the identity map in } S_A.\} \}$

### Note 26

ba1fe9df223242b5af6517275f8203bc

Given  $\alpha \in D_{2n}$ , let  $\{\{c2:: \sigma_\alpha\} \}$  denote  $\{\{c1:: \text{the permutation of } \{1, 2, \dots, n\}, \text{ representing the permutation of the vertices.}\} \}$

**Note 27**

85081cd4076348dfba43dc9e737ff07d

$D_{2n}$  acts on  $\{\{c2::\{1, 2, \dots, n\}\}$  by  $\alpha \cdot i = \{\{c1::\sigma_\alpha(i)\}\}$  for all  $\alpha \in D_{2n}$ .

**Note 28**

4a12094119574b18b849c194030d0a13

Let  $G$  be a group. Given  $g \in G$ , the map  $\{\{c2::$

$$a \mapsto ga \quad G \rightarrow G$$

$\}\}$  is called  $\{\{c1::$ left multiplication. $\}\}$

**Note 29**

99ec6293e8ff4118b8f67a8ff7d4aebf

Let  $G$  be a group written additively. Given  $g \in G$ , the map  $\{\{c2::$

$$a \mapsto g + a \quad G \rightarrow G$$

$\}\}$  is called  $\{\{c1::$ a left translation. $\}\}$

**Note 30**

0e7c694af67e4cdb98b480b89d61373f

Let  $G$  be a group. The group action of  $G$  on  $\{\{c3::$ itself $\}\}$  defined by  $\{\{c1::$

$$g \cdot a = ga, \quad \text{for all } g, a \in G$$

$\}\}$  is called  $\{\{c2::$ the left regular action of  $G$  on itself. $\}\}$

**Note 31**

a97e2c6daab04e188a70813e7ec93207

Let  $G$  be a group acting on a set  $A$ . The kernel of the action is  $\{\{c2::$ a subgroup $\}\}$  of  $\{\{c1::G.\}\}$

**Note 32**

5a1dfb95d2d14756960572225eade8e2

Let  $G$  be a group acting on a set  $A$ . Given  $\{\{c3::a \in A,\}\}$   $\{\{c1::$ the set

$$\{g \in G \mid ga = a\}$$

$\}\}$  is called  $\{\{c2::$ the stabilizer of  $a$  in  $G$ . $\}\}$

**Note 33**

40824336a8b0481394e4c7dbd2a5e12e

Let  $G$  be a group acting on a set  $A$  and  $a \in A$ . The stabilizer of  $a$  in  $G$  is  $\{\{c2::$ a subgroup $\}\}$  of  $\{\{c1::G.\}\}$

### Note 34

de72c6c8aeb345c6b825e47ed14d68d3

The kernel of an action of the group  $G$  on a set  $A$  is the same as the kernel of the associated permutation representation.

### Note 35

63892c14f75b4100b0a22a46fc813060

A group  $G$  acts faithfully on a set  $A$  if and only if the kernel of the action is the identity subgroup of  $G$ .

### Note 36

4460f313478a45de80ce8b6fea906453

Let  $V$  be a vector space over a field  $F$ . Is the action of the multiplicative group  $F^\times$  on  $V$  faithful?

Yes.

### Note 37

4f4a58eb88264a478cb3baf175b6eb3f

Let  $A$  be a nonempty set and let  $k \in \mathbb{Z}^+$  with  $k \leq |A|$ . The symmetric group  $S_A$  acts on the set of all subsets of  $A$  of cardinality  $k$  by

$$\sigma \cdot \{a_1, \dots, a_k\} = \{\sigma a_1, \dots, \sigma a_k\}$$

### Note 38

8c10a40354e149a09e1606629ecca53d

Let  $A$  be a nonempty set and let  $k \in \mathbb{Z}^+$  with  $k \leq |A|$ . The symmetric group  $S_A$  acts on the set of all ordered  $k$ -tuples of elements of  $A$  by

$$\sigma \cdot (a_1, \dots, a_k) = (\sigma a_1, \dots, \sigma a_k)$$